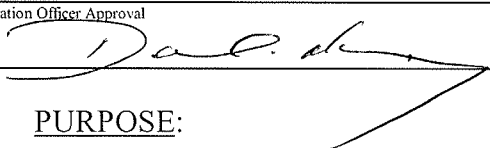




King County Information Technology Governance Policies & Standards

Policy Title Password Management Policy: Information Security and Privacy	Document Code No.
Chief Information Officer Approval 	Effective Date. February 22, 2005

1.0 PURPOSE:

To establish user and system administrator password management practices that ensure the appropriate protection of King County information assets and maintain accountability.

2.0 APPLICABILITY:

Applicable to all King County information assets, including applications and systems.

3.0 REFERENCES:

Enterprise Information Security Policy.

4.0 DEFINITIONS:

- 4.1 **Active Directory:** A directory service from Microsoft Corporation that serves as the central authority for network security, providing User Authentication and access control to network resources.
- 4.2 **Administrative Resource:** Such as routers, switches, WAN links, firewalls, servers, Internet connections, administrative-level network operating System Accounts, Active Directory and Directory Enterprise Administrative level accounts and any other IT resource.
- 4.3 **Automated Logon Process:** Storing Authentication Credentials in a registry entry, macro, or function to automatically authenticate a User to a System without User intervention.
- 4.4 **Authentication:** A security procedure designed to verify that the authorization credentials entered by a User to gain access to a network or System are valid.
- 4.5 **Authentication Credentials:** The combination of User-ID and Password.
- 4.6 **Compromised:** Something secret that is known to anyone other than the User to which the Authentication Credentials are assigned.
- 4.7 **Information Asset:** A definable piece of information, equipment, or System, that is recognized as "valuable" to the Organization that has one or both of the following characteristics:
 - Not easily replaced without cost, skill, time, resources, or a combination.
 - Part of the Organization's identity, without which, the Organization may be threatened.
- 4.8 **Organization:** Every county office, every officer, every institution, and every department, division, board and commission.
- 4.9 **Passphrase** – An exceptionally long password generally derived from a phrase or short sentence that typically eliminates spaces and replaces some letters with special

characters; for example “TheDark3stHourI\$JustBeforeDawn”. (Do not use this example.)

- 4.10 **Password:** A confidential sequence of characters used to authenticate an individual's identity, usually during a logon process.
- 4.11 **Risk Assessment:** The analysis of an Organization's Information Assets, existing controls and computer System vulnerabilities. It establishes a potential level of damage in dollars and/or other assets.
- 4.12 **Strong Password:** A Password that consists of combination of upper and lower case letters, numbers and special characters. Sometimes referred to as a “complex password”.
- 4.13 **Software:** Computer instructions or data. Anything that can be stored electronically. Software is often divided into two categories:
 - **System software:** Includes the operating system and all the utilities that enable the computer to function.
 - **Application software:** Includes programs that do real work for users. For example, word processors, spreadsheets, and database management systems fall under the category of applications software
- 4.14 **System:** Software, hardware and interface components that work together to perform a set of business functions.
- 4.15 **System Account:** A specialized User account, generally used by an operating System to start a process for an application. Accounts of this type typically have elevated privileges on the specific System running the application for which they are used.
- 4.16 **System Administrator:** The person assigned to manage and maintain a specific System. This individual usually has elevated rights and privileges on the specific System.
- 4.17 **System Password Policies:** Password policies that relate to a specific System. Due to technological limitations of specific Systems, special Password policies must be developed to ensure secure Authentication.
- 4.18 **Two-Factor Authentication:** A security process that confirms User identities using two distinctive factors – something they have and something they know. Risk of fraud is reduced by requiring two different forms of electronic identification.
- 4.19 **User:** Any individual performing work for King County utilizing a personal computer, workstation, laptop, or terminal, including but not limited to any employee, contractor, consultant, or other worker. Each term is used in the general sense and is not intended to imply or convey to an individual any employment status, rights, privileges, or benefits.
- 4.20 **User-ID:** A unique code or string of characters used to identify a specific User. Also known as User accounts

5.0 POLICIES:

- 5.1 **Mandatory Use** – Users must use a Password to validate their identity when connecting to Information Assets on the King County network.
- 5.2 **Storing Passwords** – Organizations shall require that any Authentication System (such as a x.500 compatible directory service or RADIUS, etc) that stores passwords, must store them in an encrypted format. When developing and/or acquiring Systems or Application Software Organizations shall not consider any solution that requires the storage of passwords within the system.
- 5.3 **Accountability** – Users are accountable for all activities performed under their Authentication Credentials unless an investigation proves that the User did not violate this policy at the time of the incident requiring the investigation.
- 5.4 **User Password Management**
 - 5.4.1 **Password Issuance**
 - 5.4.1.1 **Identity Authentication** - Organizations shall implement a procedure that Authenticates the identity of the User receiving a new or changed Password.
 - 5.4.1.2 **Forced Change** - Organizations shall implement a System procedure that forces the User to choose a Password before the logon process is complete when the Password is issued by a System Administrator.
 - 5.4.2 **Sharing Passwords** – Users shall keep their Password secret and shall not make their Password known to anyone else, including management, supervisors, personal assistants, human resources and System Administrators. Passwords must not be shared under any circumstance, including spoken, written, faxed, or hinted at.
 - 5.4.3 **Displaying Passwords** - Organization shall implement Systems that mask, suppress, or otherwise obscure the display of Passwords, so unauthorized parties cannot observe or subsequently recover them.
 - 5.4.4 **Changing Passwords** – Whenever possible Organizations shall implement System Password Policies that automatically force the User to change their Password at least every ninety (90) days. When automation is not possible, Users must manually change their Passwords at least every ninety (90) days. Users must also change their Password immediately after their Password or an Information Asset that they access using their Password has been, or is suspected of being, Compromised.
 - 5.4.5 **Failed Login Attempts** – When the technology allows, Organizations shall implement a process that after five (5) unsuccessful attempts to enter a Password the User-ID is disabled for at least fifteen (15) minutes unless unlocked by the System Administrator.
 - 5.4.6 **Automated Logon** - Users shall not use Passwords in any Automated Logon Process.

5.4.7 User Password Composition – Users shall use Strong Passwords and Organizations shall implement System Password Policies that require Users to choose Strong Passwords that are:

5.4.7.1 Length - At least eight (8) characters in length or the maximum length permitted by the System, whichever is shorter.

5.4.7.2 Elements - Contain at least three (3) of the following four (4) elements:

- English upper case letters: A, B, C...Z
- English lower case letters: a, b, c...z
- Westernized Arabic numbers: 0, 1, 2...9
- Special characters: { } . ' \ ` ! @ # \$ % ^ & () - (Windows)
@ # \$ (Unix, Linux, mainframe)

5.4.8 Passwords Containing User Identification – Organizations shall not assign user passwords that contain personal information, including but not limited to birthday, birth date, social security number or any part of this number, driver's license number, or employee number.

5.5 Administrative and System Account Password Management

5.5.1 Limit Password Access

5.5.1.1 Need to Know - Organizations shall limit access to administrative and System Passwords to System Administrators who have a need to know.

5.5.1.2 Store Securely - System Administrators who share an administrative or System Password shall keep the Password stored securely.

5.5.2 Changing Passwords

5.5.2.1 Change Frequency - System Administrators shall change the Password of their Administrative accounts at least every sixty (60) days. If a change frequency is not possible due to the nature of the System Account or the Administrative Resource, the Organization shall perform a Risk Assessment and develop addition security measures and provide a copy to the county information security officer.

5.5.2.2 Non-Routine Changes - System Administrators shall immediately change the Password of their Administrative account after the Password or the Administrative Resource has been, or is suspected of being, Compromised and when a System Administrator who shares this password separates from employment or changes jobs within King County. If this account is a System Account and a password change is not possible, the Organization shall perform a Risk Assessment and develop addition security measures and provide a copy to the county information security officer.

5.5.3 Password Composition - System Administrators must choose Strong Passwords for Administrative Resources that are:

5.5.3.1 Length - At least twelve (12) characters in length

5.5.3.2 **Elements** – Contains all of the following elements:

- Upper and lower case letters: A, B, C...Z, a, b, c...z
- At least four (4) numbers: 0, 1, 2...9
- At least three (3) special characters: { } . ' \ ` ! @ # \$ % ^ & ()

5.6 **Training and Awareness** – Organizations shall provide Users and System Administrators annual training on this policy and their responsibilities for Password management.

5.7 **Compliance** - Organizations shall include this policy in the annual compliance review as specified in the Enterprise Information Security Policy.

5.7.1 For each Information Asset on the King County network that requires a password that cannot comply with this policy, the Organization shall perform a Risk Assessment, implement appropriate security measures to mitigate identified risks, and provide a copy of the signed Risk Assessment to the county information security officer.

6.0 RESPONSIBILITIES:

- 6.1 **Users** comply with this policy, follow its guidelines, and understand the ramifications of all activities involving his/her User-ID and Password.
- 6.2 **System Administrators** maintain the integrity of User Passwords and Passwords for Administrative Resources, comply with this policy, and follow its guidelines.
- 6.3 **Organization Management** advise System Administrators when a User no longer needs access to a System (such as, upon termination or job change), provide training to Users reinforcing good Password management practices, and require compliance with this policy.

7.0 GUIDELINES:

7.1 **Choosing a Password** –

7.1.1 User's should **not** choose a Password that is:

7.1.1.1 Related to the User's job or personal life, such as one's work group name or favorite sports team.

7.1.1.2 Any term that could easily be guessed by someone who is familiar with the User, such as the User's name, address, date of birth, username, or nickname.

7.1.1.3 Can be easily guessed, such as "password", "welcome", etc.

7.1.1.4 Identical, or substantially similar to, a Password used by the User during the last six months.

7.1.1.5 The same Password used for a personal account outside of King County business.

7.1.2 The User should use a Passphrase whenever possible.

- 7.2 **Entering Passwords** - User should not allow another person to observe the Password as it is being entered.
- 7.3 **Sharing Passwords** - If the need arises to have access to another User's account, such as when "covering" for someone who is out of the office, contact the appropriate Information Technology (IT) organization to arrange access to the resources without sharing of the Password.
- 7.4 **Writing Down Passwords** - Avoid maintaining a paper record of Passwords. If the Password must be written down, store the paper record securely (such as in a locked cabinet or safe) or write it down in an obscure way such that it could not be recognized by anyone else as a Password.
- 7.5 **Changing Temporary Passwords** - Change a temporary Password assigned by a System Administrator at the first log-on – don't wait even if the System allows that option.
- 7.6 **System Administrator Access to User Accounts** - If a System Administrator needs access to a System as a User, the System Administrator should either (1) have the User present to enter his/her Password while performing the work, or (2) change the User's Password to a temporary Password. Once the work is complete, the System Administrator should immediately expire the temporary Password to force the User to immediately change the Password.
- 7.7 **System Accounts** – When using System Accounts where Passwords cannot be changed, the System Administrator should restrict the ability of the System Account to log in only to the specific server containing the resource for which the System Account is necessary.
- 7.8 **Authenticating Identity:** Organizations may wish to consider authenticating user identity using a courier service requiring a signature or an in-person appearance at a trusted intermediary with the provision of picture identification. Other options might include maintaining unique identifiers about users that can be verified at the time of a password change or to employ technology such as a Password self service System.
- 7.9 **Authentication for Administrative Resources** - System Administrators should employ Two-Factor Authentication for Administrative Resources.